Claims

What is claimed is:

1. A method for performing secure information processing operations utilizing a plurality of processing devices, the method comprising the steps of:

performing a setup procedure to permit interactions of a designated type to be carried out between a first participant associated with at least a first one of the processing devices and a second participant associated with at least a second one of the processing devices;

initiating in the first processing device a particular interaction with the second participant, by sending designated initiation information to the second processing device associated with the second participant, the particular interaction being configured based at least in part on one or more results of the setup procedure;

receiving as part of the interaction response information from the second processing device associated with the second participant; and

sending as part of the interaction additional information from the first processing device to the second processing device based at least in part on the received response information;

wherein the interaction is configured such that transcripts of the interaction can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction.

2. The method of claim 1 wherein the receiving and sending steps are repeated one or more times in accordance with specifications of the particular interaction.

3. The method of claim 1 wherein the first processing device comprises at least one lightweight device configured to communicate over a network with the second processing device.

4. The method of claim 1 wherein the particular interaction comprises secure mobile gaming interaction in which the first participant corresponds to a player and the second participant corresponds to a casino.

5. The method of claim 4 wherein the first processing device comprises a lightweight processing device associated with the player and the second processing device comprises at least one server associated with the casino.

6. The method of claim 1 wherein the particular interaction comprises secure mobile gaming interaction involving two or more players in which the first participant corresponds to a first player and the second participant corresponds to a second player.

7. The method of claim 1 wherein the particular interaction comprises secure contract signing interaction in which the first participant corresponds to a first party to the contract and the second participant corresponds to a second party to the contract.

8. The method of claim 1 wherein the particular interaction comprises secure digital signature exchange interaction in which the first participant corresponds to a first party to the digital signature exchange and the second participant corresponds to a second party to the digital signature exchange.

9. The method of claim 1 wherein security of the particular interaction is based at least in part on a secure probabilistic symmetric cipher (E, D) having semantic security operating in conjunction with a one-way hash function h for which collisions are intractable to find, and a commitment function C, wherein the commitment function C provides the public verifiability of designated portions of the interaction.

10. The method of claim 1 wherein the interaction is configured such that if at least one of the first and second processing devices is disconnected during the interaction, the interaction may upon reconnection of the device be continued from a designated point at or prior to the disconnection without the participants being able to alter any partial results of the interaction attributable to a portion of the interaction up to the designated point.

11. The method of claim 4 wherein the secure mobile gaming interaction comprises at least one game played by the player with the casino, the game comprising a number of consecutive rounds of one or more moves by each of the player and the casino, each of the rounds allowing the player and the casino to commit to at least one decision.

12. The method of claim 11 wherein the game is characterized by a player game tree structure associated with the player and a casino game tree structure associated with the casino, each of the game tree structures comprising a plurality of nodes, each of at least a subset of the nodes comprising a block of data that determines randomness contributed to a corresponding round of the game by the corresponding player or casino, wherein associated with each of at least a subset of the game nodes are decision preimage values that encode possible decisions to be made in the game.

13. The method of claim 12 wherein the setup procedure comprises at least the following steps:

(a) the player selecting n random numbers $d_{i1}, \ldots, d_{in}$, for each node i of the player game tree structure, and a random number r_i uniformly at random for each node, wherein each node i corresponds to a particular round of the game;

(b) the player computing for each node i a corresponding game node value $game_i = \langle h(D_{i1}, \ldots, D_{in}), R_i \rangle$, where $D_{ij} = h(d_{ij})$, $R_i = C(r_i)$, h denotes a hash function, C denotes a commitment function, and $preimage_i = (d_{i1}, \ldots, d_{in}, r_i)$ denotes a decision preimage value for $game_i$;

(c) the player computing for each node i a value which is a function of one or more of: (i) values associated with one or more of its children nodes; (ii) its corresponding game node value $game_i$; and (iii) a descriptor that identifies the game type;

(d) both the player and the casino storing information of the form $agreement_{(casino,player)}$ comprising a root value of the player game tree structure, a root value of the casino game tree structure, a hash value on a game function f_{game}, and associated digital signatures by the player and the casino.

14. The method of claim 12 wherein the secure mobile gaming interactions are implemented in accordance with a game-playing protocol comprising at least the following steps:

(a) the player initiating the game by sending a value $r_{player,cnt}$ to the casino, where *cnt* corresponds to a counter;

(b) the casino verifying that $r_{player,cnt}$ is a correct preimage to $R_{player,cnt}$, and halting the protocol if it is not the correct preimage;

(c) the casino and the player taking turns making moves in which the casino sends to the player decision preimages encoding its move, the player is presented with one or more corresponding choices via an interface at the first processing device, and a given choice selected by the player is translated into one or more preimages that are subsequently sent to the casino;

(d) step (c) being repeated one or more times in accordance with the rules of the game;

(e) the casino sending a value $r_{casino,cnt}$ to the player, which is verified correspondingly by the player;

(f) evaluating a game function f_{game} on the disclosed portions of the player and casino preimages, presenting a corresponding output to the player and the casino, and sending appropriate payment transcripts to at least one financial institution; and

(g) the player and the casino each updating the counter *cnt*, along with other state information associated with a current state of the game.

15. An apparatus for use in performing secure information processing operations, the apparatus comprising:

a memory; and

a processor coupled to the memory, the memory and processor being elements of a first processing device associated with a first participant, the processor being operative: (i) to perform a setup procedure to permit interactions of a designated type to be carried out between the first participant and a second participant associated with at least a second processing device; (ii) to initiate a particular interaction with the second participant, by sending designated initiation information to the second processing device associated with the second participant, the particular

interaction being configured based at least in part on one or more results of the setup procedure; (iii) receiving as part of the interaction response information from the second processing device associated with the second participant; and (iv) sending as part of the interaction additional information from the first processing device to the second processing device based at least in part on the received response information;

wherein the interaction is configured such that transcripts of the interaction can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction.

16. The apparatus of claim 15 wherein receiving and sending operations (iii) and (iv) are repeated one or more times in accordance with specifications of the particular interaction.

17. The apparatus of claim 15 wherein the first processing device comprises at least one lightweight device configured to communicate over a network with the second processing device.

18. The apparatus of claim 15 wherein the particular interaction comprises secure mobile gaming interaction in which the first participant corresponds to a player and the second participant corresponds to a casino.

19. The apparatus of claim 18 wherein the first processing device comprises a lightweight processing device associated with the player and the second processing device comprises at least one server associated with the casino.

20. The apparatus of claim 15 wherein the particular interaction comprises secure mobile gaming interaction involving two or more players in which the first participant corresponds to a first player and the second participant corresponds to a second player.

21. The apparatus of claim 15 wherein the particular interaction comprises secure contract signing interaction in which the first participant corresponds to a first party to the contract and the second participant corresponds to a second party to the contract.

22. The apparatus of claim 15 wherein the particular interaction comprises secure digital signature exchange interaction in which the first participant corresponds to a first party to the digital signature exchange and the second participant corresponds to a second party to the digital signature exchange.

23. The apparatus of claim 15 wherein security of the particular interaction is based at least in part on a secure probabilistic symmetric cipher (E, D) having semantic security operating in conjunction with a one-way hash function h for which collisions are intractable to find, and a commitment function C, wherein the commitment function C provides the public verifiability of designated portions of the interaction.

24. The apparatus of claim 15 wherein the interaction is configured such that if at least one of the first and second processing devices is disconnected during the interaction, the interaction may upon reconnection of the device be continued from a designated point at or prior to the disconnection without the participants being able to alter any partial results of the interaction attributable to a portion of the interaction up to the designated point.

25. The apparatus of claim 18 wherein the secure mobile gaming interaction comprises at least one game played by the player with the casino, the game comprising a number of consecutive rounds of one or more moves by each of the player and the casino, each of the rounds allowing the player and the casino to commit to at least one decision.

26. The apparatus of claim 25 wherein the game is characterized by a player game tree structure associated with the player and a casino game tree structure associated with the casino, each of the game tree structures comprising a plurality of nodes, each of at least a subset of the nodes

comprising a block of data that determines randomness contributed to a corresponding round of the game by the corresponding player or casino, wherein associated with each of at least a subset of the game nodes are decision preimage values that encode possible decisions to be made in the game.

27. An article of manufacture comprising a machine-readable storage medium for storing one or more programs for use in performing secure information processing operations utilizing a plurality of processing devices, wherein the one or more programs when executed implement the steps of:

performing a setup procedure to permit interactions of a designated type to be carried out between a first participant associated with at least a first one of the processing devices and a second participant associated with at least a second one of the processing devices;

initiating in the first processing device a particular interaction with the second participant, by sending designated initiation information to the second processing device associated with the second participant, the particular interaction being configured based at least in part on one or more results of the setup procedure;

receiving as part of the interaction response information from the second processing device associated with the second participant; and

sending as part of the interaction additional information from the first processing device to the second processing device based at least in part on the received response information;

wherein the interaction is configured such that transcripts of the interaction can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction.

28. A method for performing secure information processing operations utilizing a plurality of processing devices including at least a first processing device associated with a first participant and a second processing device associated with a second participant, the method comprising the steps of:

receiving from the first processing device in the second processing device designated initiation information initiating a particular interaction between the first participant and the second

participant, the particular interaction being configured based at least in part on one or more results of a setup procedure, the setup procedure being performed by the first participant associated with the first processing device and permitting the particular interactions to be carried out between the first participant and the second participant;

sending as part of the interaction response information from the second processing device associated with the second participant; and

receiving as part of the interaction additional information sent from the first processing device to the second processing device based at least in part on the response information;

wherein the interaction is configured such that transcripts of the interaction can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction.